EXHIBIT A

IN THE FRANKLIN COUNTY COURT OF COMMON PLEAS
GENERAL DIVISION

SONNY TRINH,

5694 Rhodes Road, Apartment 2340,
Kent, OH 44240,

on behalf of himself and all others similarly situated,

Plaintiff,

v.

MSCRIPTS, LLC,

7000 Cardinal Place,
Dublin, OH 43017,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

INTRODUCTION

1. This case is *not* about an ordinary data breach. Bad actors have obtained highly personal medical information of thousands of persons. This information is of a type that is, for many people, is precisely the information about themselves that they would most wish to keep private. And now it is no longer private.

2. Under Ohio law, every individual patient is entitled to decide for themselves how and with whom they share their medical information, if they ever share it with anyone. *See Biddle v. Warren Gen. Hosp.*, 86 Ohio St.3d 395, 408, 1999-Ohio-115, 715 N.E.2d 518 ("[I]t is for the patient—not some medical practitioner, lawyer, or court—to determine what the patient's interests are with regard to personal confidential medical information."). Every person affected by this case has been cheated of that right.

3. Defendant mscripts, LLC ("mscripts") is a pharmaceutical services provider that collects and stores vast amounts of protected health information (PHI) and personally identifying information (PII) about those obtaining prescription medications through its services. According to its promotional materials, "mscripts has become the leader in mobile pharmacy and patient engagement. . . [p]eople all over the United States use our apps to refill their prescriptions with their pharmacies [and] get information on their medications and health states through our educational tools." *See About Us*, mscripts (accessed March 9, 2023), https://mscripts.com/about-us.

4. Recognizing the highly sensitive nature of its information, mscripts promised its customers that it would "use[ ] reasonable industry standard security practices designed to protect your data from loss, misuse, unauthorized access or disclosure, alteration, or destruction." Moreover, "[t]o the extent your personal information constitutes PHI protected under HIPAA, mscripts protects PHI in accordance with the security standards required for business associates under HIPAA." *Privacy Policy* (accessed March 9, 2023). https://mscripts.com/privacy. Mscripts failed to live up to its end of the bargain.

5. According to mscripts's data breach notice, "certain files in cloud storage where accessible from the Internet without the need for authentication . . ." Moreover, this information had been publicly accessible for six years—from September 30, 2016 to November 18, 2022.

6. The information that was accessible to anyone with an internet connection was highly sensitive--"[t]he files that were accessible included prescription order summaries related to locker pickups at participating pharmacy locations and images of prescription bottles and insurance cards submitted by pharmacy patients through the mscripts® web or mobile app."

7. Plaintiff Sonny Trinh is a victim of the data breach. Mscripts collected his PHI and PII via the mscripts app while making use of the Meijer Pharmacy. As a result of mscripts's failure to take reasonable precautions, Trinh's PHI and PII was exposed to anyone with an internet connection, thereby subjecting him to a severe invasion of privacy.

8. Trinh, on behalf of himself and all others similarly situated, seeks damages and equitable relief for mscripts' negligence, breach of confidence, breach of contract, and (alternatively) unjust enrichment.

9. Trinh and the Class are entitled to judgment in an amount exceeding $25,000. *See* CIV. R. 8(A).

PARTIES

10. Plaintiff Sonny Trinh is a resident of Kent, Ohio.

11. Defendant mscripts, LLC is a private company with its principal place of business located at 7000 Cardinal Place, Dublin, Ohio 43017. Mscripts is owned by Cardinal Health, which has its principal place of business in Franklin County.

JURISDICTION AND VENUE

12. Mscripts is subject to this Court's personal jurisdiction because its principal place of business is (and at all relevant times was) located in Dublin, Ohio.

13. This Court has subject-matter jurisdiction under R.C. 2305.03 because this is a civil case in which the amount-in-controversy exceeds $15,000.

14. Venue is proper in the Franklin County Court of Common Pleas because the Defendant's principal place of business is located in this county and, on information and belief, the Defendant's relevant acts and omissions occurred at its principal place of business. *See* CIV. R. 3(C)(2)–(3)

FACTUAL ALLEGATIONS

A. Mscripts collects sensitive data about its customers.

15. Mscripts produces a platform, centered around the mscripts app, that allows patients to manage their pharmaceutical subscriptions. *See Pharmacy Platform*, mscripts (accessed March 9, 2023), https://mscripts.com/what-we-do/pharmacy-platform.

16. In connection providing those services, mscripts creates and stores PHI and PII concerning its customers. This PHI includes pharmaceutical prescriptions, originating pharmacy, and health insurance information. *Notice of Data Breach*, Exhibit 1.

17. Mscripts also creates and stores PII, including name, date of birth, and address. *Id.*

18. Mscripts's business model requires that customers provide PHI and PII in order to use the mscripts platform. Mscripts's thus, at a minimum, indirectly monetizes its customers, and by extension its customers' PHI and PII.

B. Mscripts promised to keep patients' PHI secure.

19. Mscripts publishes a Privacy Policy, which "describes the personal information that we collect from you, how we use that personal information, and to whom we disclose it." *Privacy Policy*, at ¶ 1.

20. In addition, "[t]his Privacy Policy forms part of, and is hereby incorporated into, the mscripts Terms of Service." *Id.* at 11. As such, the Privacy Policy is part of the contractual relationship between mscripts and its users, and "[t]he User must indicate express consent to the Terms of Service in order to use the mscripts Service." *Terms of Service* (accessed March 9, 2023). https://mscripts.com/terms.

21. The notice of privacy practices is a binding term of the contract, in that it gives both parties certain enforceable legal rights over the patients' information. For example, the contract allows mscripts to use customers' information "to create aggregate-level data that we may publish in reports and marketing materials about the Service." *Privacy Policy*, at ¶ 3.

22. Under the terms of the contract, mscripts has a legal duty to "use[ ] reasonable industry standard security practices designed to protect your data from loss, misuse, unauthorized access or disclosure, alteration, or destruction ." *Id.* at ¶ 6.

23. The agreement further states that "[t]o the extent your personal information constitutes PHI protected under HIPAA, mscripts protects PHI in accordance with the security standards required for business associates under HIPAA." *Id., at* ¶ 6. Therefore, mscripts is contractually obligating itself to its customers to follow best practices outlined under HIPAA.

24. On information and belief, the relevant portions of this contract—which was effective May 1, 2016—applies to all class members. *Id.* at ¶ 12.

C. It was highly foreseeable that a third-party would attempt to access mscripts's data.

25. Given the type of data mscripts collected and stored, it was highly foreseeable that bad actors would attempt to access mscripts's systems.

26. "[H]ackers are likely to be drawn to databases containing information which has a high value on secondary black markets," such as "identifying and financial data" or "intimate and health-related data." Mark Verstraete & Tal Zarsky, *Optimizing Breach Notification*, 2021 U. ILL. L. REV. 803, 854–55 (2021). Consequently, "relevant and rational firms should engage in greater security investment and reduced collection—all steps to limit the prospects of a potential breach and subsequent notification." *Id.* at 855.

27. Companies in the healthcare industry frequently create and store identifying, financial, and health-related data.

28. Perhaps unsurprisingly, then, "the healthcare industry has faced the highest number of [data] breaches among all industries." Adil Hussain Seh, et al., *Healthcare Data Breaches: Insights and Implications*, 8 HEALTHCARE 133, 2 (2020), https://bit.ly/3QcL4Ng.

29. Data breaches are a well-known threat in the healthcare industry. According to the American Medical Association, "cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care." Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://bit.ly/3mKAf7O.

30. Mscripts stored financial, identifying, and health-related information on its systems.

31. Therefore, it was highly foreseeable that a bad actor would seek to access data concerning Trinh's and the Class that was stored on mscripts's systems.

D. As a result of mscripts's failure to implement reasonable data security practices, cybercriminals accessed patients' PHI and PII.

32. At some point in late 2022, mscripts "learned that certain files in cloud storage were accessible from the Internet without the need for authentication between September 30, 2016 and November 18, 2022." *Notice of Privacy Incident*, (accessed March 16, 2023). https://www.mscripts.com/notice-of-privacy-incident.

33. Said another way, for over a six-year period, mscripts's left its sensitive information *completely exposed* to any individual with an internet connection.

34. According to the Notice of Privacy Incident, customers of many local pharmacies (including but not limited to Giant Eagle, Costco, Fresh Market, and Meijer) who utilized the mscripts platform had their personal information exposed.

35. More specifically, according to the Notice of Privacy Incident, the information exposed included:

a. The names of affected customers;

b. "Order summary – date of birth, phone number, address, and prescription number;"

c. "Prescription information – address, prescription number, medication name, and/or originating pharmacy information;"

d. "Health insurance information – insurance company, member ID, group number, and/or dependents' names, if any."

36. Given that the above information was subject to no security protocols of any kind for a period of over six years, it is reasonable to believe that mscripts's customers had their information compromised by cybercriminals at some point during the exposed period.

37. Moreover, because the information is of a particularly sensitive and valuable nature, it is reasonable to infer that the hackers will use victims' data for fraudulent purposes.

38. The Notice of Privacy Incident provided no explanation for why this information was exposed for this long, how such an egregious lapse in security could occur, and what was done to address this problem beyond unspecified "measures."

39. In addition, no compensation was offered to affected mscripts's customers.

40. On information and belief, mscripts failed to adequately train its employees on even the basic cybersecurity protocols, including:

a. Effective password management and encryption protocols, including, but not limited to, the use of multi-factor authentication for all users;

b. Locking, encrypting and limiting access to computers and files containing sensitive information;

c. Implementing guidelines for maintaining and communicating sensitive data;

d. Protecting sensitive patient information, including personal and financial information, by implementing protocols on how to request and respond to requests for the transfer of such information and how to securely send such information through a secure file transfer system to only known recipients; and

e. Providing focused cybersecurity awareness training programs for employees.

41. The FTC has noted the need to factor data security into all business decision-making. *Start With Security, A Guide for Business*, FTC (accessed June 9, 2022), https://bit.ly/3mHCGYz. According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software. *Id.*

42. To that end, the FTC has issued orders against businesses that failed to employ reasonable measures to secure sensitive payment card data. *See In the matter of Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) ("[Defendant] allowed users to bypass authentication procedures" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks, such as employing an intrusion detection system and monitoring system logs."); *In the matter of DSW, Inc.*, No. C-4157, ¶ 7 (Mar. 7, 2006) ("[Defendant] failed to employ

sufficient measures to detect unauthorized access."); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008) ("[R]espondent stored . . . personal information obtained to verify checks and process unreceipted returns in clear text on its in-store and corporate networks[,]" "did not require network administrators . . . to use different passwords to access different programs, computers, and networks[,]" and "failed to employ sufficient measures to detect and prevent unauthorized access to computer networks . . ."); *In the matter of Dave & Buster's Inc.*, No. C-4291 (May 20, 2010) ("[Defendant] failed to monitor and filter outbound traffic from its networks to identify and block export of sensitive personal information without authorization" and "failed to use readily available security measures to limit access between instore networks . . ."). These orders, which all preceded the data breach, further clarify the measures businesses must take to meet their data security obligations.

43. On information and belief, mscripts's use of outdated and insecure computer systems and software that are easy to hack, and its failure to maintain adequate security measures and an up-to-date technology security strategy, demonstrates a willful and conscious disregard for privacy, and has exposed the PHI of Plaintiff and thousands of members of the proposed Class to unscrupulous operators, con artists, and outright criminals.

44. Mscripts violated its obligation to implement best practices and comply with industry standards concerning computer system security. Mscripts failed to comply with security standards and allowed its patients' PHI and PII to be accessed and stolen by failing to implement security measures that could have prevented or mitigated the data breach.

D. Trinh's information was exposed in the data breach.

45. Sonny Trinh was a mscripts customer by and through utilizing the Meijer Pharmacy services. Via that relationship, mscripts created records of Trinh's's PHI and PII.

46. Mscripts required Trinh to provide his PHI and PII as a condition of using the mscripts service.

47. Trinh believed, as part using the mscripts service pursuant to the Terms of Service, that his PHI and PII would be kept secure. Had Trinh known that mscripts did not utilize reasonable data security measures, he would have utilized different platforms.

48. Indeed, mscripts affirmatively promised to do more than the bare minimum to protect Trinh's PHI, and Trinh reasonably expected that mscripts would uphold its end of the bargain.

49. On or about February 13, 2023, Trinh received a data breach notification from mscripts informing him that his PHI and PII had been exposed.

50. None of this would have occurred if mscripts had implemented reasonable data security precautions.

E. Trinh and the Class suffered legally cognizable injuries as a result of mscripts's negligence.

51. Trinh and the Class suffered at least six concrete injuries as a direct and proximate result of their information being exposed.

1. Invasion of Privacy

52. *First*, Trinh and the Class suffered an invasion of privacy.

53. When it comes a breach of PHI, an injury *has already occurred* because the victim inherently suffered a privacy injury.

54. Privacy injuries are concrete. As Justice Brandeis once observed, an invasion of privacy can subject victims "to mental pain and distress, far greater

than could be inflicted by mere bodily injury." Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

55. Medical data breaches cause privacy injuries because they expose inherently private information to the public without consent. Indeed, "[p]atients are highly sensitive to disclosure of their health information," particularly because PHI "often involves intimate and personal facts, with a heavy emotional overlay." Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 621 (2002). Unsurprisingly, then, empirical evidence demonstrates that "[w]hen asked, the overwhelming majority of American patients express concern about the privacy of their medical records." Sharona Hoffman & Andy Podgurski, *E-Health Hazards: Provider Liability and Electronic Health Record Systems*, 24 BERKLEY TECH. L.J. 1523, 1557 (2009).

56. This information is highly sensitive, and Trinh's privacy was invaded when his PHI was accessed without his permission.

57. Trinh's—like any reasonable person similarly situated—experienced extreme distress and anxiety upon learning that his privacy had been invaded in this manner.

2. Identity Theft

58. *Second*, Trinh and the Class will suffer injuries due to an increased likelihood of identity theft.

59. According to experts, one out of four data breach notification recipients become a victim of identity fraud. *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, THREATPOST.COM (Feb. 21, 2013), https://bit.ly/3zB8Uwv.

60. Stolen PHI is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service,

stolen PHI can be worth up to $1,000.00 depending on the type of information obtained. *See* Brian Stack, *Here's How Much Your Personal Information is Selling for on the Dark Web*, EXPERIAN (Dec. 15, 2017), https://bit.ly/2Ox2SGY.

61. The value of Plaintiff's and the proposed Class's PHI on the black market is considerable. Stolen PHI trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

62. It can take victims years to spot identity or PHI theft, giving criminals plenty of time to milk that information for cash.

63. One such example of criminals using PHI for profit is the development of "Fullz" packages. "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record or more on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See, e.g.*, Brian Krebs, *Medical Records For Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://bit.ly/3Qj2eJd.

64. Cyber-criminals can cross-reference two sources of PHI to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

65. The development of "Fullz" packages means that stolen PHI from the data breach can easily be used to link and identify it to Plaintiff's and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PHI stolen by the cyber-criminals in the data breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and other members of the proposed Class's stolen PHI is being misused, and that such misuse is fairly traceable to the data breach.

66. According to the FBI's Internet Crime Complaint Center (IC3) 2019 Internet Crime Report, Internet-enabled crimes reached their highest number of complaints and dollar losses that year, resulting in more than $3.5 billion in losses to individuals and business victims.

67. Further, according to the same report, "rapid reporting can help law enforcement stop fraudulent transactions before a victim loses the money for good." Defendant did not rapidly report to Plaintiff and the Class that their PHI had been stolen.

68. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

69. In addition to out-of-pocket expenses that can exceed thousands of dollars for the victim of new account identity theft, and the emotional toll identity theft can take, some victims have to spend a considerable time repairing the damage caused by theft of their PHI. Victims of new account identity theft will likely have to spend time correcting fraudulent information in their credit reports and continuously monitor their reports for future inaccuracies, close existing bank/credit accounts, open new ones, and dispute charges with creditors.

70. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiff and the Class will need to be remain vigilant against unauthorized data use for years or even decades to come.

3. Loss of Time

71. *Third*, Trinh and the Class have been forced to spend time responding to the data breach.

72. Trinh spent considerable time reviewing the data breach notification and considering how best to protect what was left of his privacy.

73. Trinh has also retained counsel to pursue this matter, which necessarily took up more of his time, and was reasonably necessary to respond to the breach.

74. Trinh and the Class also spent time reviewing the data breach notification.

75. Trinh and the Class are likely to spend more time responding to the data breach in the future, particularly in light of the severe risk of future identity theft.

4. Diminished Value of Personal Information

76. *Fourth*, the breach has diminished the value of Trinh and the Class's personal information.

77. The Federal Trade Commission ("FTC") has recognized that consumer data is a new and valuable) form of currency. In an FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that "most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency." *Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable*, FTC (Dec. 7, 2009), https://bit.ly/3xKfzmu.

78. Trinh and the Class's information has already been accessed by criminals, which decreases its utility.

79. Therefore, the value of Trinh's and the Class's personal information was reduced by the data breach.

5. Mitigation Damages

80. *Fifth*, mscripts's failure to notify Trinh and the Class of the breach within a reasonable time prevented them from mitigating further damages.

81. If Trinh and the Class had known about the above injuries sooner, they could have taken precautions to protect themselves from future damages.

82. Because they were delayed from taking protective measures, Trinh and the Class are now at a greater risk than if they had been able to take precautions.

6. Benefit of the Bargain

83. *Sixth*, Trinh and the Class were denied the benefit of their bargain with mscripts.

84. Trinh and the Class entered into a contractual agreement with mscripts to receive services.

85. Mscripts will only provide services to customers who agree to provide PHI and PII.

86. Trinh and the Class provided mscripts with their PHI and PII.

87. Mscripts explicitly promised that it would take reasonable precautions to safeguard that PHI and PII.

88. Mscripts did not take reasonable precautions to safeguard Trinh and the Class's PHI and PII, and it did not notify them of the data breach within a reasonable time.

89. Therefore, Trinh and the Class were denied the benefit of their bargain with SOMC.

CLASS ACTION ALLEGATIONS

90. Pursuant to CIV. R. 23(b)(3), Plaintiff seeks certification of a class defined as follows:

> All individuals who received a Notice of Privacy Incident from mscripts, llc, dated February 9, 2023, stating that they had their Personal Identifying Information or Personal Health Information exposed.

91. Excluded from the Class are: (a) mscripts and its officers, directors, legal representatives, successors and wholly or partly owned subsidiaries or affiliated companies; (b) class counsel and their employees; and (c) the judicial officers and their immediate family members and associated court staff assigned to this case.

92. *Ascertainability*. The Class can be readily identified through mscript's records, which is demonstrated by the fact that mscripts has already identified the class members and notified them of the breach. *Notice of Data Breach*, Exhibit 1.

93. *Numerosity*. At least 66,372 mscripts customers had their information exposed in the breach. *See* "mscripts Cloud Storage Misconfiguration Exposed PHI for 6 Years," The HIPAA Journal *https://www.hipaajournal.com/mscripts-cloud-*

storage-misconfiguration-exposed-phi-for-6-years/ (accessed March 9, 2023). Therefore, the Class is so numerous that individual joinder is impracticable.

94. *Typicality*. Plaintiff's claims are typical of the Class he seeks to represent. Like all class members, Plaintiff's personal information was exposed as a result of mscripts's failure to implement reasonable data security measures. Thus, Plaintiff's claims arise out of the same conduct and are based on the same legal theories as those of the absent class members.

95. *Adequacy of Class Representative*. Plaintiff will fairly and adequately protect the interests of the Class. He is aware of his fiduciary duties to absent class members and is determined to faithfully discharge his responsibility. Plaintiff's interests are aligned with (and not antagonistic to) the interests of the Class.

96. *Adequacy of Counsel*. In addition, Plaintiff has retained competent counsel with considerable experience in class action and other complex litigation, including data breach cases. Plaintiff's counsel have done substantial work in identifying and investigating potential claims in this action, have considerable knowledge of the applicable law, and will devote the time and financial resources necessary to vigorously prosecute this action. They do not have any interests adverse to the Class.

97. *Commonality and Predominance*. This case presents numerous questions of law and fact with answers common to the Class that predominate over questions affecting only individual class members. Those common questions include:

a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiff and the Class's PHI;

b. Whether Defendant breached the duty to use reasonable care to safeguard the Class's PHI;

c. Whether Defendant breached its contractual promises to safeguard Plaintiff and the Class's PHI;

d. Whether Defendant knew or should have known about the inadequacies of its data security policies and system and the dangers associated with storing sensitive PHI and PII;

e. Whether Defendant failed to use reasonable care and commercially reasonable methods to safeguard and protect Plaintiff and the Class's PHI and PII from unauthorized release and disclosure;

f. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiff and the Class's PHI and PII from unauthorized release and disclosure;

g. Whether the data breach was caused by Defendant's inadequate cybersecurity measures, policies, procedures, and protocols;

h. Whether Defendant took reasonable measures to determine the extent of the data breach after it was discovered;

i. Whether Defendant is liable for negligence, gross negligence, or recklessness;

j. Whether Defendant's conduct, practices, statements, and representations about the data breach of the PHI and PII violated applicable state laws;

k. Whether Plaintiff and the Class were injured as a proximate cause or result of the data breach;

l. Whether Plaintiff and the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiff and the Class;

m. Whether Defendant's practices and representations related to the data breach breached implied warranties;

n. What the proper measure of damages is; and

o. Whether Plaintiff and the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

98. *Superiority and Manageability*. A class action is superior to individual adjudications because joinder of all class members is impracticable, would create a risk of inconsistent or varying adjudications, and would impose an enormous burden on the judicial system. The amount-in-controversy for each individual class

member is likely relatively small, which reinforces the superiority of representative litigation. As such, a class action presents far fewer management difficulties than individual adjudications, preserves the resources of the parties and the judiciary, and protects the rights of each class member.

CAUSES OF ACTION

Count 1: Negligence

99. Plaintiff incorporates by reference all of the above allegations.

100. Plaintiff and the Class entrusted their PHI and PII to Defendant. Defendant owed to Plaintiff and other the Class a duty to exercise reasonable care in handling and using the PHI and PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the data breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

101. Defendant owed a duty of care to Plaintiff and the Class because it was foreseeable that Defendant's failure to adequately safeguard their PHI and PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI and PII—just like the data breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff and the Class's PHI and PII failing to properly supervise both the manner in which the PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen. Indeed, Defendant acknowledged its duty to safeguard this information in its own privacy policies.

102. Defendant owed to Plaintiff and the Class a duty to notify them within a reasonable time frame of any breach to the security of their PHI. Defendant also owed a duty to timely and accurately disclose to Plaintiff and the Class the scope, nature, and occurrence of the data breach. This duty is necessary in order for

Plaintiff and the Class to take appropriate measures to protect their PHI and PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps in an effort to mitigate the harm caused by the data breach.

103. Defendant owed these duties to Plaintiff and the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff and the Class's personal and financial information and PHI and PII for medical treatment services. Plaintiff and the Class were required to provide their personal information and PHI and PII to Defendant in order to receive medical treatment and services from Defendant, and Defendant retained that information.

104. The risk that unauthorized persons would attempt to gain access to the PHI and PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PHI and PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PHI and PII.

105. PHI and PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PHI and PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

106. Defendant breached its duties by failing to provide any security of any kind with regard to the personal information and PHI and PII of Plaintiff and the Class, which actually and proximately caused the data breach and Plaintiff and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the data breach to Plaintiff and the Class, which actually and proximately caused and exacerbated the harm from the data breach and Plaintiff and the Class's injuries-in-fact.

107. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and the Class's actual, tangible, injury-in-fact and damages, including, without limitation, theft of their PHI by criminals, improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the data breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

Count 2: Negligence Per Se

108. Plaintiff incorporates by reference all of the above allegations.

109. Defendant is a "business entity" that maintains, stores, or manages computerized data that includes "personal information" as defined by R.C. § 1349.19(A).

110. Plaintiff and the Class's PHI includes "personal information" as defined by R.C. § 1349.19(A).

111. Defendant was aware of a breach of its computer system that it believed or reasonably should have believed had caused or would cause loss or injury.

112. Defendant had an obligation to disclose the data breach to Plaintiff and the Class in a timely fashion as mandated by R.C. §§ 1349.19(B)(1)-(2).

113. Defendant had a duty to Plaintiff and the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiff and the Class's PHI and to notify Plaintiff and the Class if the security of their PHI was compromised.

114. Defendant breached its duties to Plaintiff and the Class under R.C. §§ 1349.19(B)(1)-(2) by failing to provide fair, reasonable, adequate, or timely notice of the data breach to Plaintiff and the Class.

115. Defendant's failure to disclose the data breach in a timely manner as required by R.C. § 1349.19(B) constitutes negligence per se.

116. As a direct and proximate cause of Defendant's negligence in failing to timely notify them of the data breach, in violation of R.C. § 1349.19(B), Plaintiff and the Class sustained actual losses and damages as described in this complaint.

117. Defendant is also a health care provider who transmits health information in electric form and therefore is a "covered entity" under HIPAA. 45 C.F.R. § 160.103.

118. As a covered entity, Defendant is subject to the Data Breach Notification Rule. 45 C.F.R. § 164.404(a)(1).

119. This data breach exposed unsecured protected health information.

120. Defendant owed a duty to provide individual notice of that breach "without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. 45 C.F.R. § 164.404(b).

121. Defendant claims to have discovered the breach on or about November 2022, but it did not notify affected individuals until February 9, 2023—a delay of at least three months.

122. This delay was unreasonable under the circumstances.

123. The Data Breach Notification Rule reveals the proper standard of care for an entity such as Defendant with respect to notification for data breaches such as this one.

124. Defendant failed to meet that standard of care.

125. As a direct and proximate result, Plaintiff suffered actual losses and damages.

Count 3: Negligent Invasion of Privacy

126. Plaintiff incorporates by reference all of the above allegations.

127. "Ohio recognizes the tort of negligent invasion of the right of privacy." *Herman v. Kratche*, 8th Dist. No. 86697, 2006-Ohio-5938, ¶ 41, citing *Prince v. St. Francis-St. George Hospital, Inc.*, 20 Ohio App. 3d 4, 7, 484 N.E.2d 265 (1st Dist. 1985). *Accord, e.g.*, *Hanus v. McNeely*, 5th Dist. No. CA-9277, 1993 Ohio App. LEXIS 5823, *7–8; *Sowards v. Norbar, Inc.*, 78 Ohio App. 3d 545, 555, 605 N.E.2d 468 (10th Dist. 1992).

128. Defendant violated Plaintiff and the Class's right to privacy in two ways.

129. First, Defendant negligently caused an intrusion upon Plaintiff and the Class's seclusion.

130. Plaintiff and the Class's PHI is highly sensitive. Any reasonable person feel outrage or shame if their medical information was exposed without permission.

131. An unauthorized third-party accessed Plaintiff and the Class's PHI, thereby intruding upon their seclusion.

132. This third-party was only able to access that medical information Defendant failed to reasonably safeguard Plaintiff and the Class's PHI.

133. Therefore, Defendant is liable for negligent intrusion upon seclusion.

134. Second, Defendant negligently caused a disclosure of private facts concerning Plaintiff and the Class.

135. Plaintiff and the Class's PHI contains highly sensitive information relating to their private lives. Any reasonable person would feel shame or outrage if their medical information were publicly disclosed.

136. Because Defendant provided no security whatsoever for Plaintiff and the Class's PHI, it is highly like that a third-party accessed Plaintiff and the Class's PHI without their authorization. Therefore, there has been a public disclosure of private facts.

137. Any reasonable person would find it highly offensive that Plaintiff and the Class's PHI was publicly disclosed.

138. The disclosure would not have happened but-for Defendant's negligence.

139. The public has no legitimate interest in accessing medical information of Plaintiff and the Class.

140. Therefore, Defendant is also liable for negligent disclosure of private facts.

141. Plaintiff and the Class suffered damages a direct and proximate result of Defendant's misconduct.

Count 4: Breach of Confidence

("*Biddle*" Claim)

142. Plaintiff incorporates by reference all of the above allegations.

143. Under Ohio law, "an independent tort exists for the unauthorized, unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship." *Biddle v. Warren Gen. Hosp.*, 86 Ohio St.3d 395, 1999-Ohio115, 715 N.E.2d 518, paragraph 1 of syllabus.

144. Mscripts collected medical information from Plaintiff and the Class in connection with their patient-physician relationship.

145. This information was non-public and, indeed, highly confidential.

146. Plaintiff and the Class were unable to protect the data they had entrusted to mscripts, and thus were in a relationship of dependence and trust.

147. That data was disclosed to a third party through mscripts's systems without authorization from Plaintiff and the Class.

148. That third-party was only able to access Plaintiff and the Class's medical information because mscripts negligently and recklessly disregarded its duty to preserve the confidentiality of its patients' medical information.

149. Plaintiff and the Class suffered damages as a direct and proximate result of Defendant's breach of confidence.

Count 5: Breach of Contract

150. Plaintiff incorporates by reference all of the above allegations.

151. Defendant offered to provide services to Plaintiff and the Class.

152. Defendant also required Plaintiff and the Class to provide Defendant with their PHI in order to receive services.

153. Defendant received valuable consideration from the provision of services to Plaintiff and the Class members.

154. Plaintiff and the Class accepted Defendant's offer by providing PHI and PII to Defendant in exchange for receiving Defendant's services, pursuant to mscripts Terms of Service.

155. Defendant expressly promised to protect customers' PHI by implementing safeguards over and above the bare minimum.

156. Defendant implicitly promised to extend the same protection to customers' PII.

157. Plaintiff and the Class would not have entrusted their PHI to Defendant in the absence of such agreement with Defendant or if they had known that Defendant would not adequately protect it.

158. Defendant materially breached the contract(s) it had entered with Plaintiff and the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into its computer systems that compromised such information. Defendant further breached the implied contracts with Plaintiff and the Class by:

a. Failing to properly safeguard and protect Plaintiff and the Class's PHI and PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PHI that Defendant created, received, maintained, and transmitted in violation of 45 C.F.R. § 164.306(a)(1)

159. The damages sustained by Plaintiff and the Class as described above were the direct and proximate result of Defendant's material breaches of its agreement(s).

160. Plaintiff and the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

161. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

162. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

163. Defendant failed to advise Plaintiff and the Class of the data breach promptly and sufficiently.

164. Defendant failed to provide adequate data security, even though it knew that Plaintiff and the Class understood Defendant would safeguard their PHI and PII and would not have provided it to Defendant absent such understanding.

165. In these and other ways, Defendant violated its duty of good faith and fair dealing.

166. Plaintiff and the Class have sustained damages as a result of Defendant's breaches of the agreement.

PRAYER FOR RELIEF

167. Plaintiff, individually and on behalf of all others similarly situated, hereby demands:

a. Certification of the proposed Class;

b. Appointment of the undersigned counsel as class counsel;

c. An award of all damages, including attorneys' fees and reimbursement of litigation expenses, recoverable under applicable law;

d. Restitution or disgorgement of all ill-gotten gains; and

e. Such other relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

168. Plaintiff demands a jury trial on all applicable claims.

Respectfully submitted,

By: /s/ *Matthew R. Wilson*

MEYER WILSON CO., LPA
Matthew R. Wilson (72925)
Email: mwilson@meyerwilson.com
Jared W. Connors (101451)
Email: jconnors@meyerwilson.com
305 W. Nationwide Blvd.
Columbus, Ohio 43215
Telephone: (614) 224-6000
Facsimile: (614) 224-6066

TURKE & STRAUSS LLP
Samuel J. Strauss (*pro hac vice* to be filed)
sam@turkestrauss.com
Raina Borrelli (*pro hac vice* to be filed)
raina@turkestrauss.com
613 Williamson St., #201
Madison, WI 53703
P: (608) 237-1775

Counsel for Plaintiff and the Proposed Class